AMENDMENTS TO THE CLAIMS

1 - 13 (Cancelled)

14. (New) A method of operating a computer system comprising a first node connectable to a second node by way of any of a plurality of gateway nodes, wherein:
(a) the first node initially establishes a first virtual private network (VPN) connection with the second node by way of one of the gateway nodes, using a session key which is held in a cache store in the first node to encrypt communications between the first node and said one of the gateway nodes;
(b) the first node monitors said one of the gateway nodes for failure;
(c) in the event of failure of said one of the gateway nodes, the first node deletes the session key from the cache store and searches the cache store to determine whether another session key has been cached allowing a new VPN connection to be established with the second node by way of another of the gateway nodes;
(d) in the event that another session key has not been cached, the first node initiates a key establishment protocol exchange with a selected one of the gateway nodes, other than the failed node, to establish a new session key allowing a new VPN connection to be established with the second node by way of said selected one of the gateway nodes, the new session key being saved in the cache store.

15. (New) A method according to claim 14, wherein said selected one of the gateway nodes is chosen randomly from the plurality of gateway nodes.

16. (New) A method according to claim 14, wherein the first node monitors said one of the gateway nodes for failure by periodically sending a failure detection signal to said one of the gateway nodes and determining whether a response to the failure detection signal is received from said one of the gateway nodes within a predetermined time.

17. (New) A method according to claim 16, wherein the failure detection signal is transmitted when a respective message encryption key has been established and no communication from the selected one of the gateway nodes has been received by the first node within a predetermined time interval.

18. (New) A method according to claim 16, wherein transmission of the failure detection signal is deferred until after the first node has transmitted encrypted communications to the selected one of the gateway nodes.

19. (New) A method according to claim 16, wherein the failure detection signal is transmitted as an encrypted packet.

20. (New) A computer system comprising a first node connectable to a second node by way of any of a plurality of gateway nodes, wherein the first node comprises:
(a) a cache store for storing session keys;
(b) means for establishing a first virtual private network (VPN) connection with the second node by way of one of the gateway nodes, using a session key held in the cache store to encrypt communications between the first node and said one of the gateway nodes;
(c) means for monitoring said one of the gateway nodes for failure;
(d) means operative in the event of failure of said one of the gateway nodes, for deleting the session key from the cache store and searching the cache store to determine whether another session key has been cached allowing a new VPN connection to be established with the second node by way of another of the gateway nodes;
(e) means operative in the event that another session key has not been cached, for initiating a key establishment protocol exchange with a selected one of the gateway nodes, other than the failed node, to establish a new session key allowing a new VPN connection to be established with the second node by way of said selected one of the gateway nodes, and for saving the new session key in the cache store.